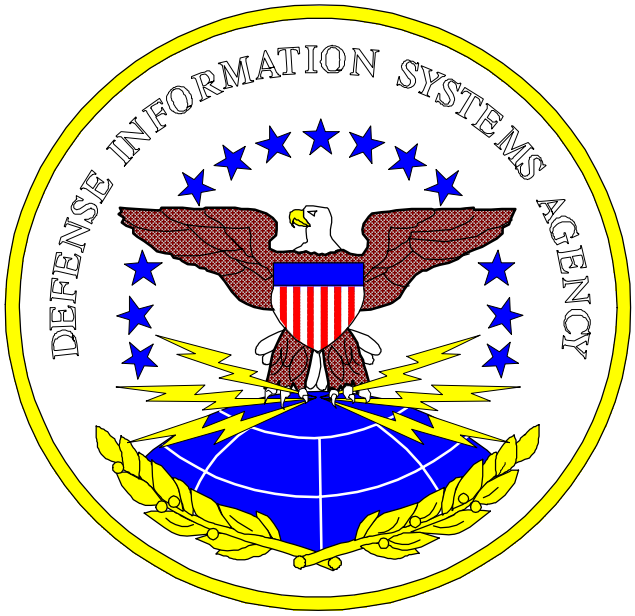

DoD Medium Assurance PKI Major Directory Challenges

LCDR Paul Friedrichs

Defense Information Systems Agency

PKI Chief Engineer

friedrip@ncr.disa.mil

8 October 1998

DoD Medium Assurance PKI Technical Objectives

- **Purely standards-based**
  - **Support multiple applications and products**
- **Support digital signature and encryption**
- **Provide functional separation**
  - **Support legal non-repudiation**
  - **Support data recovery**
- **COTS-based**
  - **Possible outsource of elements**
- **Support FIPS-compliance requirements**

Client Support For Multi-Valued Directory Attributes

- **Two Certificates**
  - **keyUsage: digitalSignature, nonRepudiation**
  - **keyUsage: digitalSignature, keyEncipherment & e-mail address in certificate subject (migrating to subjectAltName)**
- **But clients only use first certificate written to directory**
  - **DAP, LDAP and proprietary clients**
- **Forced to duplicate entire directory service !**
- **Need to get the word out to client developers !**

X.500 Data Model Entries

- **Naming and directory manageability conflict**
  - **All requirements must be satisfied with *one* hierarchy**
    - **(not the purpose of hierarchical object classes)**
  - **Uniquely name (currently by DIT territory)**
  - **Meaningfully name (DN components)**
    - **Often need to violate territory**
  - **Manage information**
    - **Delegation**
    - **Management instructions at top of each subtree**
    - **But subtrees selected to meaningfully name subjects ?**
  - **Users need to find information**
    - **User should not need to see DIT - should just be UI challenge**
      - **Provide the user any view *they* need**
    - **Index across subtrees (used to satisfy management requirements)**

X.500 Data Model Entries

- **Separate hierarchy for each conflicting requirement ?**
  - **Possible kluges of the technology within a domain:**
    - **Unique leaf RDNs - drag and drop entries to ease management**
      - **Possibly only certify RDN within domain**
    - **Place all information on central server and index across domain**
      - **Allows web UI that supports *user's* needs**
    - **Possibly still allows a standard interface to the rest of the world**
- **Performance (location, push-pull, cache) optimized separately ?**

X.500 Data Model Attributes

- **Need to delegate *attribute* management**
  - **DIT is perpendicular to organizations' requirements**
  - **This is why we're seeing "meta-directories"**
    - **Different management requirements for each group of attributes**
    - **For shared set of "entries"**
  - **Technology invisible to management requirements**
    - **Possibly reflect each group in a separate DIT**
      - **Using unique RDN as key between management DITs**
    - **Change in management for group of attributes reflected only once**
      - **At the top of each subtree**
  - **Internal management architecture invisible to outside**
    - **Possibly still allows standard interface to the rest of the world**

Directories

- **Schema-aware clients vs. three-tier C/S authentication**
- **D*elegation* appears to be directory's greatest strength**
  - **Not necessarily *distribution***
- **Directories are all about politics**
  - **The technology must thrive in, not ignore, politics**
- **Separate central, local and community directory services ?**
- **Scalability primarily requires *scalable manageability***
- **Clients must support multi-valued attributes !**